Technical Disclosure Commons

Defensive Publications Series

July 2020

SECURE USB PRINTING

HP INC

Secure USB Printing

Abstract:

Users always seek convenience while doing a job and printing is no exception. Amongst the available printing methods such as print through driver, pull printing, e-print, stored job printing, USB printing, USB printing has been developed as one of the most convenient and preferred way of printing by the users. The reason for USB print gaining popularity is because user can carry the printable job in a USB storage device, go to any printer, printer and select which document to print using the front panel and print. One of the primary attributes that differ USB print to other printing mechanisms is it doesn't require internet connectivity. While there are many advantages of USB printing, it carries a disadvantage of low or no security with it. This abstract discusses about a security problem involved with USB printing and the solution to address that.

Problem Statement:

In USB printing users need to carry a USB device with the printable document in it and must connect it to the printer to retrieve the job and print. With this flow user often tends to forget to remove the USB storage device after printing. In such scenario, if user is using a public printer, the data content can be accessed or tempered by unauthorized users.

To address this issue, there are mechanisms available which remind/notify the user to disconnect the USB device to continue with the printing. In this process, the data from the USB device is copied to the printer's local storage and then the print job is executed. There are two major issues exist in this flow.

1. The data that is copied to the local storage are generally unencrypted and can be accessed by unauthorized user even if the user has removed the USB device. Although, the data is flushed out from the local storage after successful execution of print jobs, there is no such mechanism available for the scenarios when printer entering error state before job completion or printer's firmware crash. In these scenarios, the data remains in the printer's memory and are exposed to unauthorized access.
2. If printer enters an error state before job completion, the user will have to again connect the USB device to proceed with printing. In this scenario, printer will again start printing from the first page and the pages which were printed earlier would be wasted.
3. If user pause the job before its completion. it exposes a security threat to be accessed from unauthorized users. As the data is copied locally to the printer and no security in it, to protect, either user must complete the job or delete the job. If user pause the job with the intention of resuming it later, it can be accessed by anyone.

This paper addresses the above-mentioned security flaws and makes the user's experience better.

Prior Solution:

There is no prior solution available for this problem.

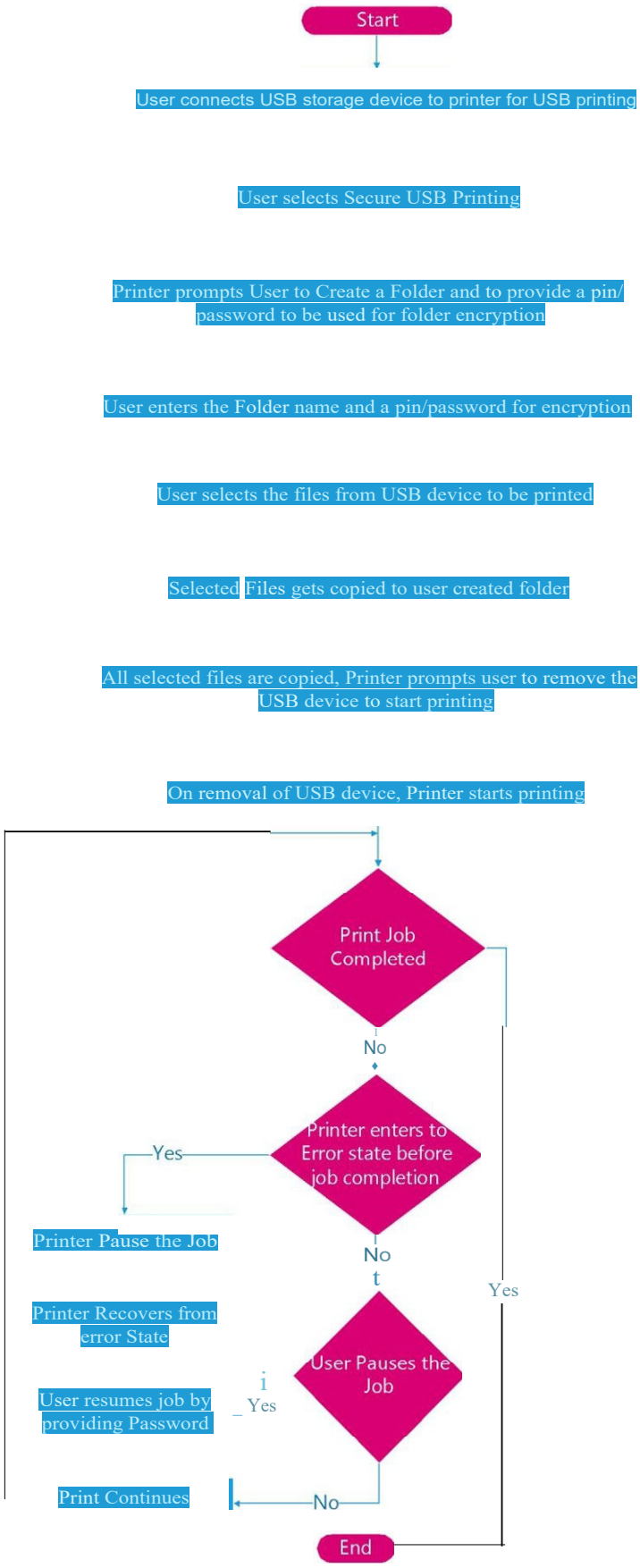
Solution:

In the existing secured USB printing solution, the printable documents are copied from the USB device to the printer's local storage and the user is prompted to disconnect the USB device to proceed

with printing. The copied data is flushed out of the memory once the job is printed successfully. However, if the printer enters a bad state before the job completion, the temporary folder that contains the printable documents are vulnerable to unauthorized access which is a security flaw in the flow. Our solution discusses a series of steps that will ensure that USB printing is completely secured and provides a better user experience.

The broad sequence of operations carried out during this process are as follow:

1. User connects the USB device to the printer.
2. Regular printing and secured printing options can be configured on the printer.
3. If secured printing option is enabled on the printer, the user is prompted to create a temporary folder, where all the files that the user selects to print from USB are to be copied. After the folder creation, the user is prompted to provide a pin or password for the folder (user needs to remember the PIN if it intends to access the folder again in future). Once the user has created a folder and has assigned it a PIN or password, the printable content, that user wants to print from USB is copied to the created folder.
4. The user is prompted to remove the USB device via a message on the front panel to proceed with printing.
5. Once user removes the USB storage device, printer starts printing.
6. In scenarios when printer enter error state due to events like paper jam, out of paper, out of ink, firmware crash or any other printer errors, the job is paused
7. As the folder is encrypted, any unauthorized user will not be able to access the content or even trigger the print job if printer recovers from error state.
8. Whenever, the printer recovers from the error state, the user can resume the print job. To resume the paused print job, user will be prompted to enter the PIN or password which it had entered at the time of creating the folder. Once user enters the valid PIN or password, the printer resumes printing the remaining pages.
9. After the completion of the print job, the copied job with the folder is erased from the memory.
10. The above steps are depicted in the flow chart below.


Start
User connects USB storage device to printer for USB printing
User selects Secure USB Printing
Printer prompts User to Create a Folder and to provide a pin/ password to be used for folder encryption
User enters the Folder name and a pin/password for encryption
User selects the files from USB device to be printed
Selected Files gets copied to user created folder
All selected files are copied, Printer prompts user to remove the USB device to start printing
On removal of USB device, Printer starts printing
Print Job Completed
No
Printer enters to Error state before job completion
Yes
Printer Pause the Job
No
t
Yes
Printer Recovers from error State
User Pauses the Job
User resumes job by providing Password
i
Yes
Print Continues
No
End

Advantages:

1. This solution provides end to end security in USB printing.
2. This solution improves the user experience and saves print media and ink in scenarios of printer error by providing a resume print mechanism without compromising the security and reduces the printing cost.
3. If user is printing any large confidential document, the user needs to be around the printer to collect the printed documents, and if for some reason the user needs to pause the job, the user is left with only option of cancelling the print job. With this solution, the user can pause the print job and go. The user can come back to printer anytime and resume the print job by entering the PIN or password. This solution provides a great user convenience and experience with complete security.
4. As the copied files from the USB device are kept in an encrypted folder, the files remain safe in case of firmware crash or hard-disk theft which ensures complete protection of user's data.
5. The user will not have to carry the USB device again to print the same job which was left incomplete the last time because of the printer error, as the job is kept securely in the printer's memory. The job is flushed out of the printer's memory only when all the pages in the document is printed successfully.

Disclosed by Avasthi Abhishek and Pradhan Puranjaya, HP Inc.